

Signature Verification in Health Care

The health care industry today is under ever-increasing pressure to conduct more and more of its business electronically:

- Market forces require firms to drive cost and inefficiency from their outmoded paper-based processes, and to make more information available to consumers and business partners online.
- Litigation risks compel firms to devote more attention to data integrity and to the adoption of practices which ensure accountability of those who create and access data.
- Regulations increasingly permit or even require firms to create and maintain records electronically, while adopting stringent measures to protect that information from unauthorized access or alteration.

Biometric signature verification technology from Vector Intelligence, Inc. can play a major role in meeting both the business and regulatory needs of the health care industry for enhanced data security.

Electronic Signatures in FDA-Regulated Industries

FDA regulations at 21 CFR Part 11, enacted in 1997, permit and encourage the use of electronic signatures and recordkeeping in the industries it regulates (human and veterinary pharmaceuticals, personal care products, medical devices, food and beverages). While the FDA does not mandate the use of electronic processes, firms adopting electronic recordkeeping must do so in a manner that satisfies the agency's requirements, including those for an electronic signature.

The agency has been enforcing Part 11 aggressively since January, 2000. The FDA notes that packaged software should be designed with Part 11 in mind, and should have built-in tools for capturing electronic signatures and creating secure electronic records. The FDA does not regard ordinary UserID/Password log-ins as compliant, because there is no assurance that the person performing or verifying an operation subject to Part 11 is in fact the same person who logged in.

The Prescription Drug Marketing Act

In 1999, the FDA promulgated 21 CFR Part 203 to implement the requirements of the Prescription Drug Marketing Act of 1987. The regulations require that certain prescription drug wholesalers provide a "pedigree" to purchasers identifying each prior sale of a drug. Like Part 11, Part 203 creates opportunities for providers of products and services that would generate an irrefutable electronic pedigree for drug distributors; such a solution will obviously need to include user authentication and data integrity measures.

The HIPAA Challenge

The Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates new security standards to protect an individual's health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses, and health plans. HIPAA also mandates that a new electronic signature standard be used where an electronic signature is employed in the transmission of a HIPAA standard transaction. Although final rules have not yet been adopted, the security and electronic signature standards proposed at 45 CFR Part 142 are likely to be adopted without substantial modification, and to become effective in 2002. The new standards are intended to protect the confidentiality, integrity, and availability of individual health information. The electronic signature standard in particular is intended to provide a reliable method of assuring message integrity, user authentication, and non-repudiation.*

The importance of reaching HIPAA compliance quickly and completely is difficult to overstate. As a Gartner Group Analyst observed, "When provisions of HIPAA take effect in October 2002, the fine for improper handling of patient data will rise to a maximum of \$50,000 per incident, which can go higher if done under false pretenses or done with the intent to sell, transfer, or use the information. For a provider with thousands of patient records, the cost of even a minor slipup could quickly reach millions of dollars."

Biometric Signature Verification: An Important Part of Your Compliance Program

Signature verification technology from VII can play an important role in meeting these and other compliance challenges. Although BioSig can be deployed in many ways, depending on the requirements of the application or organization, at its core it is an authentication technology: it accurately confirms a user's identity by comparing a reference file, typically generated when the user enrolls in the system, with a signature file that must be created anew each time authentication is required. The reference file (and, theoretically, the verification engine) can be stored remotely in a secure server, or locally on a handheld computer, PC or smart card, as needs dictate. The signature file created at the point of authentication contains time stamp data, and like the reference file, is stored in an encrypted form that contains no useful or intelligible information about the appearance of the signature or any of its characteristics. Verification can be performed over a network (open or closed) or on the same device used to capture the signature file.

Successful user authentication can trigger a range of possible consequences, such as granting access to data (or even to physical facilities), or embedding a signature (with or without its visual counterpart) in an electronic document, thereby creating virtually incontestable evidence of when and by whom the document was signed, and preventing that document from being further edited. BioSig is an excellent supplement to or substitute for alphanumeric passwords (the most problematic form of authentication today), including those employed in Public Key cryptography. Since the final rules under HIPAA are likely to mandate adoption of PKI and digital signatures,

* Electronic signature is defined as "the attribute affixed to an electronic document to bind it to a particular entity. An electronic signature secures the user authentication (proof of claimed identity) at the time the signature is generated; creates the logical manifestation of signature (including the possibility for multiple parties to sign a document and have the order of application recognized and proven); supplies additional information such as time stamp and signature purpose specific to that user; and ensures the integrity of the signed document to enable transportability of data, interoperability, independent verifiability, and continuity of signature capability. Verifying a signature on a document verifies the integrity of the document and associated attributes and verifies the identity of the signer." 45 CFR § 142.310.

institutions and application developers pursuing HIPAA compliance should give strong consideration to technologies that can improve upon PKI's traditional, but problematic, dependence on passwords, and biometric signature verification is, in many settings, the least expensive, least intrusive, and most administratively practical choice among all the options.

Applications have already been developed incorporating BioSig to meet the same demands imposed by HIPAA and the other regulations facing the health care industry today. The Galactic Access service, from InterNetEx, employs BioSig to authenticate and lock electronic documents. Documents signed within Galactic Access are—among other features and characteristics—authenticated, encrypted, unalterable, time-stamped, and subject to non-repudiation.

The Business Case for Electronic Recordkeeping in Health Care

The use of paper-intensive procedures within the health care industry today is pervasive, but imposes staggering costs while generating errors that cause delay, expense, and in some cases, actual physical harm to patients. For many mission-critical applications within the industry (e.g., writing prescriptions, entering treatment orders at a hospital, and patient discharge and bill review, to name a few), electronic recordkeeping, supported by biometric signature verification, should be carefully considered because it can help to meet patient care objectives in a way that is cost-effective, promotes best practices, and is acceptable to health care providers, insurers and patients alike.

The cost savings from adoption of electronic processes can be impressive. On average, paper-based insurance claims take 60 days until receipt of payment at a cost of about \$5 per claim; payment for a clean electronic claim only takes 14 days at about \$.25 to \$.30 per claim. The Department of Health and Human Services predicts that the savings gained through transaction standardization could be as high as \$29.9 billion over 10 years.

But the benefits of electronic transactions extend well beyond mere cost savings. Consider the problem of patient care order entry in hospitals. Typically today, a nurse or physician leaves the patient's location and orders additional treatment at a potentially distant location. While the procedure is automated, it is also problematic: the practitioner may be distracted or delayed on the way to the terminal, or may make data entry errors (in an extreme case, even designating the wrong patient). By contrast, a practitioner equipped with a handheld computer, operated at the bedside, can ensure that the patient is not left alone during order entry, that the order is entered within moments of the practitioner's decision, and that it is entered for the correct patient (thanks to an identifying bar code on the bedside or even the patient's ID tag). In this setting, signature verification requires no additional hardware (all handheld and tablet computers can deploy BioSig), making it the most natural form of security to employ.

Similarly, consider the patient discharge and bill review scenario. Today's bill review/discharge process is long and drawn-out. Before charges can be submitted to the insurer, the patient must review and approve a lengthy chart of treatments, examinations and prescriptions. Poor recordkeeping results in insurance disputes and delays, and drives up the hospital's administrative costs. Insurance-related disputes and delays can even force patients to delay follow-up care. But presenting bills to the patient in electronic form, and collecting the patient's signature electronically, not only speeds the process, it generates a virtual "paper trail" that can reduce disputes with the hospital or insurer, and their attendant costs and delays.

The drug prescription system is also ripe for change. Today, over two billion prescriptions are written each year, the majority in handwriting, on a prescription pad by a doctor within the

confines of his office. Not only does this system require accurate interpretation by the pharmacist, but it requires multiple data entry points if the additional drug is to become a part of the patient's permanent health record. The Business Roundtable Health and Retirement Taskforce estimates that 500,000 serious medication mistakes could be avoided each year through automated prescription systems, which would remove the difficulties of reading doctor handwriting, warn against contraindications for specific drug treatments—and, incidentally, largely eliminate the trade in illicit drugs linked to stolen (paper) prescription pads. Clearly, electronic prescriptions offer tremendous advantages over their paper counterparts, but only if protected by strong authentication measures; and what could be more simple and natural than preserving the signature process, but simply substituting one surface (an electronic pad) for another (paper)?

Contact Us

Call today to learn more about the role that biometric signature verification can play in your own applications or business processes.

Joel E. Simkins
Chief Marketing Officer
Vector Intelligence, Inc.
604 S. Washington Sq. #1003
Philadelphia, PA 19106

(215) 923-5942
jsimkins99@earthlink.net